August 2001

International Standard ISO/IEC 17799:2000
Information Security Management,
Code of Practice for Information Security Management

Frequently Asked Questions

Introduction

The National Institute of Standards and Technology's (NIST's) Information Technology Laboratory developed this Frequently Asked Questions (FAQ) in response to the high level of interest in this activity. The FAQ addresses a number of questions being asked by persons in both government and industry about ISO/IEC 17799:2000, *Code of Practice for Information Security Management*. This document is for background information purposes only and does not serve as an official US Government position.

ISO/IEC 17799:2000, *Code of Practice for Information Security Management*, was published as an international standard in late 2000. The British Standards Institution (BSI) had submitted the document for international standardization via the ISO/IEC JTC 1 fast track process. Any P-member of JTC 1 or organization in Category A liaison with JTC 1 may propose that an existing standard from any source be submitted without modification directly for vote as a Draft International Standard (DIS). The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide. The original BSI document was British Standard (BS) 7799-1, with same title. DIS 17799 was subsequently approved by a majority of the ISO/IEC National Bodies (NBs) in the fall of 2000. It was published by ISO/IEC as International Standard 17799. Many procedural and substantive content objections were raised against it both before and since approval. An immediate revision process has now been started in response to these substantial objections.

While ISO/IEC 17799:2000 is an international standard, it is considered by many NBs with the largest IT markets to be technically flawed or incomplete. Serious questions have also been raised about potential inappropriate use in conjunction with a supposed "ISO certification" process for organizations.

What is ISO/IEC 17799:2000?

The stated purpose of ISO/IEC 17799:2000 is to *"give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."*

What does ISO/IEC 17799:2000 cover?

As a general organizational information security management guide, ISO/IEC 17799:2000 is not intended to give definitive details or "how-to's". Rather, it addresses topics in terms of policies and general good practices. The document specifically identifies itself as "a starting point for developing organization specific guidance." It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. Given such caveats, the document in 65 pages briefly addresses the following major topics:

- Establishing organizational security policy,
- Organizational security infrastructure,
- Asset classification and control,
- Personnel security,
- Physical and environmental security,
- Communications and operations management,
- Access control,
- Systems development and maintenance,
- Business continuity management, and
- Compliance.

What does ISO/IEC 17799:2000 NOT cover?

ISO/IEC 17799:2000 is not a technical information security manual. It provides general guidance on the wide variety of topics listed above, but typically does not go into depth. It takes the "broad brush" approach. So 17799 does not provide definitive or specific material on any security topic.

As discussed below, 17799 does not provide enough information to support an in-depth organizational information security review, much less a certification program. However, 17799 certainly could be useful as a high-level overview of information security topics that could help senior management to understand the basic issues involved in each of the topic areas. Several nations have indicated that portions of 17799 are in conflict with their national laws, particularly those covering privacy.

How does ISO/IEC 17799:2000 relate to crypto, digital signatures or PKI interoperability?

The general guidance approach taken by 17799 includes some information related to crypto matters. However, there is not enough information given in the document to support the development or management of operational crypto programs, such as PKI interoperability. For example, here is the ***complete*** content of the document's coverage of PKI (in section 10.3.5.2):

"In addition to the issue of securely managed secret and private keys, the protection of public keys should also be considered. There is a threat of someone forging a digital signature by replacing a user's public key with their own. This problem is addressed by the use of a public key certificate. These certificates should be produced in a way that uniquely binds information related to the owner of the public/private key pair to the public key. It is therefore important that the management process that generates these certificates can be trusted. A certification authority normally carries out this process, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust. The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 4.2.2)."

Note that NIST Special Publication (SP) 800-21, Guideline for Implementing Cryptography in the Federal Government, is available for free download. This SP contains practical guidance on setting up various crypto-related organizational security programs. See:

http://csrc.nist.gov/publications/nistpubs/index.html.

How does ISO/IEC 17799:2000 relate to British Standard 7799?

BS 7799 is a two-part security management standard that was developed by the British Standards Institution (BSI) and has been used extensively in the United Kingdom (UK), under sponsorship of the UK government. The two parts of BS 7799 are:

- 7799-1 (Part 1): *Code of Practice for Information Security Management*, is a UK national standard for a code of practice for information security management. BS 7799-1 is ***not*** a specification for an organizational information security management program, which they refer to as an "Information Security Management System" (ISMS) and therefore ***cannot*** be used for certification purposes. Note that the current version of ISO/IEC 17799 (prior to its planned immediate revision) is entirely based on BS7799-1.
- 7799-2 (Part 2): *Specification for Information Security Management Systems*, a supporting checklist of security controls. The UK considers that BS7799-2 ***is*** a specification for an ISMS and could be used as the basis for accredited certification. This document has ***no*** direct relationship to ISO/IEC 17799.

BSI submitted BS 7799-1 to ISO/IEC JTC 1 in early 2000 for balloting under the ISO/IEC JTC 1 Fast-Track Processing. Any P-member of JTC 1 or organization in Category A liaison with JTC 1 may propose that an existing standard from any source be submitted without modification directly for vote as a Draft International Standard (DIS). The criteria for proposing an existing standard for the fast-track procedure is a matter for each proposer to decide. ***Note that the contents of BS 7799 had previously been submitted to ISO/IEC JTC 1 a few years earlier in normal fashion as a new work item, but it was then rejected upon balloting.***

How does ISO/IEC 17799:2000 relate to ISO/IEC 15408:1999, the Common Criteria for IT Security Evaluation?

The short answer is that there is **no** close connection in either subject matter or approach between the Common Criteria standard (ISO/IEC 15408:1999) and ISO/IEC 17799: 2000. They do not cover the same or similar subject matter.

The Common Criteria standard is intended to support the specification and technical evaluation of IT security features in products (and ultimately in installed systems, although that part has not been developed yet). Normally, the products are evaluated as part of the development/production cycle. The Common Criteria standard also has a major usage as a structure, syntax and catalog of information technology specifications that can be used to describe user technical requirements for security in products.

ISO/IEC 17799: 2000, on the other hand, is not a technical standard, but a management standard, and deals with an examination of the non-technical issues relating to installed IT systems. These issues have to do with such matters as personnel, procedural, and physical security, and security management in general.

That being said, it is useful to note that IT security products and systems specified and evaluated under the Common Criteria can be very helpful in ensuring the success of an organizational security program, as their use can significantly reduce the security risk faced by the organization. To see how the Common Criteria can help organizations face their security challenges, please refer to NIST Special Publication 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, which can be downloaded at the following website;

http://csrc.nist.gov/publications/nistpubs/index.html

Is there a Part 2 of ISO/IEC 17799:2000, as there is of the UK's BS 7799?

BSI did not submit BS 7799-2, the security controls checklist, to ISO/IEC JTC 1 for standardization, possibly for reasons alluded to in the response to the question below about "irregularities." There is no indication at this time whether they will do so. At this time, ISO/IEC JTC 1 has no plans to generate a 17799-2 itself as a future work item.

Is an ISO-approved ISO/IEC 17799:2000 system security certification program available, like the ISO 9000 process quality certification program?

ISO/IEC 17799:2000 is a code of practice or information security management guideline that does not provide the necessary level of detail to support such a program. As noted above, there is no companion 17799 Part 2 to provide detailed conformance specifications for an organizational information security management program. Until such time as such a specification document might become accepted as an ISO/IEC JTC 1 standard, there is ***no*** possibility of an "official ISO" 17799-certification program such as

exists with ISO 9000. While some may choose to use BS 7799-2 informally in conjunction with IS 17799 (or, far more appropriately, with BS 7799-1) to do some form of system security "certification," this ***cannot*** be construed as a true ISO certification. It is important to observe that the formally recognized certification schemes that are currently known to exist today in various nations provide certification against BS 7799-2 and ***not*** ISO/IEC 17799:2000.

What complaints have been made regarding "irregularities" surrounding approval of ISO/IEC 17799:2000?

ISO/IEC 17799:2000 was adopted over the objection of some NBs with significant IT markets. A significant number of the NBs actively participating in the security standardization work within ISO/IEC JTC 1 SC 27 (IT Security Techniques) have complained about the DIS fast track balloting during the summer of 2000. The complaints of irregularities include: acceptance of late ballots that provided the necessary favorable margin, counting of an apparently negative ballot as a positive one, refusal of the DIS ballot resolution meeting to consider the many substantive technical comments submitted during balloting, irregularly speedy publication of the document as an ISO/IEC JTC 1 standard once the balloting was closed, and other matters. The National Bodies of Germany, France and Canada have lodged strong official protests to ISO/IEC central authorities about these irregularities. Canada has recently filed 28 formal "defect reports" on the content of 17799. The US NB considered lodging a similar protest but did not do so; instead it supported the other protests.

Who voted for and against DIS 17799 during the fast-track process?

BSI, the UK national standards body, voted in favor. They were joined by Australia, the Netherlands, Brazil, and fourteen other NBs. The NBs opposing adoption were Belgium, Canada, France, Germany, Italy, Japan and the US. ***Note that all six of the NBs representing "G-7" major economic nations, other than the UK, were unified in opposing adoption of the draft.***

What is the US position on ISO/IEC 17799:2000?

The US position submitted in June 2000 on DIS 17799 opposed its adoption for many substantive technical reasons. Most of the members of the US Technical Advisory Groups (TAGs) for ISO/IEC JTC 1 and ISO/IEC JTC 1 SC 27 represent US industry. While there was no official US government position expressed, US TAG members from both the Commerce Department (via NIST) and Department of Defense (via DISA) supported US position. The current US position is strongly in favor of an early major revision of the document, properly taking into account the negative technical comments submitted on it during the summer 2000 fast-track balloting process.

Why was the US position against ISO/IEC 17799:2000?

Here are the main points of concern about 17799 that the US NB expressed in comments submitted with its fast-track ballot response of June 2000:

1. There is no compelling reason for an International Standard at this time in the difficult-to-quantify area of computer security "code of practice". The "code of practice" area is better served by guidance documents, such as the existing ISO/IEC "Guidelines for the management of IT Security (GMITS)" series of technical reports.
2. While DIS 17799 is valuable as a self-assessment and improvement tool, it is not acceptable as a standard because it does not have the necessary measurement precision of a technical standard.
3. While DIS 17799 appears to be a good document, describing one useful security approach, there is no indication that it is inherently more technically sound or better for the purpose of providing general guidelines for security management than other "code of practice" materials that are also widely available, some of which are already ISO documents. [Various other widely accepted security management documents, including several from NIST, were listed as examples.]
4. It is noted that much of the useful security management information available in the documents noted above is not contained in DIS 17799, so if DIS 17799 were to become an international standard it would be unacceptably incomplete.
5. The short time available in this "fast track" process is inadequate to fully analyze the implications of DIS 17799 in the context of its utility as the international baseline standard on computer security. In comparison, it is noted that the GMITS series, with similar content, has been under development in the international community for many years, with much discussion and evolution during that time.

What is NIST's position regarding ISO/IEC 17799:2000?

NIST has supported the original and current US NB position on the document. An overwhelming majority of US government and industry members of the US Technical Advisory Groups (TAGs) for ISO/IEC JTC 1 and ISO/IEC JTC 1 SC 27 supported these positions.

In addition to the reservations expressed in the US NB comments above, there is also a concern about the high cost of ISO/IEC 17799:2000, which is available from ISO and BSI. In contrast, NIST continues to make available ***at no charge*** a large number of highly useful documents that are supportive of an effective organizational information security program. See next answer.

What NIST documents could be used instead of ISO/IEC 17799:2000?

Check out the wide variety of helpful security publications available at the NIST website:

http://csrc.nist.gov/publications/nistpubs/index.html.

Numerous guidance documents can be freely downloaded there. In the NIST Special Publication 800-series, the US NB identified the following documents as particularly useful for organizational information security management:

- SP 800-12, Computer Security Handbook
- SP 800-14, Generally Accepted [Security] Principles & Practices
- SP 800-18, Guide for Developing Security Plans

The following additional documents in the SP 800-series should also be very helpful:

- SP 800-23, Guide to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- (Draft SP 800-26), Self-Assessment Guide for IT Systems

What ISO/IEC documents could be used instead of ISO/IEC 17799:2000?

The ISO/IEC TR 13335 Guidelines for the Management of IT Security (GMITS) series of Technical Reports are particularly useful. Most are presently available from ANSI.

To order, go to ANSI at:

http://www.ansi.org/

Then go to the NSSN and document search:

http://www.nssn.org/search.html

In "Find this document number" enter "13335" and the following information is available for buying the GMITS series of Technical Reports:

Document Number: ISO/IEC TR 13335-1:1996
Title: Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
$54.00

Document Number: ISO/IEC TR 13335-2:1997
Title: Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security
$46.00

Document Number: ISO/IEC TR 13335-3:1998
Title: Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
$92.00

Document Number: ISO/IEC TR 13335-4:2000

Title: Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
$105.00

ISO/IEC DTR 13335-5 is not yet available from ANSI:

Document Number: ISO/IEC DTR 13335-5
Title: Information technology -- Guidelines for the management of IT Security – Part 5: Management guidance on network security

Some of these Technical Reports are now under revision. Status information on revisions is available from NCITS T4:

http://www.ncits.org/tc_home/t4htm/index.htm

Go to Technical area - List of projects and look for TR 13335. The best way to get the latest copies of these revisions would be to join NCITS T4 (See the last question.).

What is the current status of ISO/IEC 17799:2000 as an international standard?

While some National Bodies consider 17799 to be a legitimate international standard, others do not. The National Bodies' technical and procedural complaints mentioned above have not yet been fully addressed by ISO/IEC authorities to the satisfaction of those bodies. Therefore, there is no true consensus at this time regarding 17799.

In partial response to the concerns expressed, ISO/IEC JTC 1 is presently balloting a strongly backed proposal to begin an immediate revision of 17799 in order to accommodate the many technical objections lodged against it. The proposal includes:

- Request the SC27 Secretariat to commence a NB letter ballot to seek approval for an early revision and to distribute this document (SC 27 N2877) with this letter ballot.
- Ensure that the revision take account of the Canadian Defect Reports as contained in SC 27 N2821-2847 and the NB comments that were submitted as part of the fast track ballot process.

- Request the SC27 Secretariat to issue a call for contributions as part of any revision initiative and nominations for a project editor.

This open revision process is probably the only way that widespread consensus could be reached on the document. As another encouraging sign, ISO/IEC JTC 1 SC 27/ WG 1 participants recently approved an acting editor from Germany (Oliver Weisman) for the proposed 17799 revision project and will conduct an open selection process for a permanent new project editor.

As a US person, how can I participate in the ISO/IEC 17799:2000 revision process?

The US TAG to ISO/IEC JTC 1 SC 27 is the National Committee for Information Technology Standards (NCITS), Technical Committee T4, Security Techniques. Technical Committee T4, Security Techniques, participates in the standardization of generic methods for information technology security. This includes development of: security techniques and mechanisms; security guidelines; security evaluation criteria; and identification of generic requirements for information technology system security services. As the US TAG to ISO/IEC JTC 1 SC27, T4 provides recommendations on US positions to the JTC 1 TAG.

Fees for voting members and advisory members on NCITS Technical Committees (including one Alternate) are $800 per year. The Chairman of NCITS Technical Committee T4 is Rowena Chester, University of Tennessee. Send email to Rowena Chester at:

mailto:roc2@cornell.edu

The NCITS Technical Committee T4 web site is:

http://www.ncits.org/tc_home/t4.htm

Membership information for NCITS and the JTC 1 TAG are available on their websites.

The NCITS web site is:

http://www.ncits.org/

The US Technical Advisory Group to JTC 1 (JTC 1 TAG) web site is:

http://www.jtc1tag.org/